UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,726	03/31/2004	Jesse Lipson	4023-001	9869

64843 7590 10/07/2010

TRIANGLE PATENTS, P.L.L.C.
P.O. BOX 28539
RALEIGH, NC 27611-8539

EXAMINER	
ZIA, SYED	
ART UNIT	**PAPER NUMBER**
2431	
MAIL DATE	**DELIVERY MODE**
10/07/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/814,726	LIPSON, JESSE	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8, 12-15, 19- 25, 27-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,12-15,19-25 and 27-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment and remarks filed May 12, 2010. Claims 1-8, 12- 15, 19- 25, 27-39 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 12, 2010 has been entered.

Response to Arguments

Applicant's arguments filed May 12, 2010 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1, 2, 3, 5, 12, 22, and 23 applicants argued that the cited prior arts (CPA) [Takagi et al. (U.S. Patent 6,396,926 B1)] Takagi describes a method of encryption that generates a squareful modulus as the product of a series of distinct prime factors wherein one of the prime factors is raised to an exponent k, thus generating a product from non-distinct prime factors. Takagi then teaches the decryption of the encoded message using all of the distinct prime

factors. The present invention, instead, teaches the generation of a squarefree modulus and the decryption of the resulting encoded message using less than all of the distinct prime factors. The claims have been amended to distinguish over the prior art".

This is not found persuasive. The system of cited prior art teaches a cryptographic method in authentication system that involves the method of obtaining encrypted sentence based on preset relationship between predefined secret and public representation key values. The encrypted sentence is obtained based on preset relationship between secret values (p1,p2...pN) and public representation key values (p1,k1, p2,k2..pNkN) and other public representation key values (e) and secret key values (d). In the system of cited prior art, public representation key N is the product of the secret key values and k values where k is positive integer. Then public representation key values are calculated based on predefined relationship between secret key values and public representation key values (Fig.1-5, and col.13 line 45 to col.17 line 15).

As a result, the system of cited prior art does implement and teaches a public key cryptography schemes to allow for decryption of messages using less than all of the prime factors of the modulus that is used for encryption of the messages.

Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the

examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 1-8, 12-15, 19-25, 27-39 are respectfully maintained.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-8, 12-15, 19-25, 27-39 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-8, 12-15, 19-25, 27-39 are rejected under 35 U.S.C. 101 based on Supreme Court precedent and recent Federal Circuit decisions, a 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In re Bilski et al, 88 USPQ 2d 1385 CAFC (2008); Diamond v. Diehr, 450 U.S. 175, 184 (1981); Parker v. Flook, 437 U.S. 584, 588 n.9 (1978); Gottschalk v. Benson, 409 U.S. 63, 70 (1972); Cochrane v. Deener, 94 U.S. 780,787-88 (1876).

An example of a method claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the apparatus that accomplishes the method steps, or positively recite the subject matter that is being transformed, for example by identifying the material that is being changed to a different state.

Here, applicant's method steps are not tied to a particular machine. Thus, the claims are non-statutory.

The mere recitation of the machine in the preamble with an absence of a machine in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 12-15, 19-25, 27-39 are rejected under 35 U.S.C. 102(b) as being anticipated by Takagi et al. (U.S. Patent 6,396,926 B1).

1. Regarding Claim 1, Takagi teach and describe a system for encrypting/decrypting messages, comprising: a public key cryptosystem further comprising a computer operable for generating keys for use with messages that have been encrypted and/or decrypted wherein the public key cryptosystem having a predetermined number of prime factors used for the generation of a modulus N and an exponent e; wherein the modulus N is not a squareful number; wherein a proper subset of the prime factors of the modulus N composed of less than all of the distinct prime factor, along with the exponent e, are required to decrypt messages that are encrypted using the public exponent e and the public modulus N, where e and N are calculated using RSA methods, and encryption occurs using RSA methods (Fig.1-5, and col.13 line 45 to col.17 line 15).

2. Regarding Claim 2, Takagi teach and describe a method for encrypting/decrypting messages comprising the steps of: providing a public key cryptosystem including a computer operable to generate at least one key for encrypting/decrypting at least one message, the public key cryptosystem having a predetermined number of prime factors used for the generation of a modulus N and an exponent e; wherein the modulus N is not a squareful number; wherein a proper subset of the prime factors of the modulus N composed of less than all of the distinct prime factor are required to decrypt messages that are encrypted using the public exponent e and the public modulus N, where e and N are calculated using RSA methods, and encryption of the message occurs using RSA methods (Fig.1-5, and col.13 line 45 to col.17 line 15)..

3. Regarding Claim 3, Takagi teach and describe a method for encrypting/decrypting messages comprising the steps of: encrypting on a computer a plaintext message M into a ciphertext message C using any method that produces a value equivalent to C=M.sup.e mod N, where 0.ltoreq.M<N.sub.d, such that the ciphertext C can be decrypted into the plaintext message M using only e and the prime factors of N.sub.d N being the product of all of the numbers in the set S; N is not a squareful number;S being a set of at least two prime numbers, p.sub.1 . . . p.sub.k, where k is an integer greater than 1; e being a number; S.sub.d being a proper subset of S composed of less than all of the distinct prime factor; N.sub.d being the product of all of the numbers in the set S.sub.d (Fig.1-5, and col.13 line 45 to col.17 line 15).

4. Regarding Claim 5, Takagi teach and describe a method for decrypting encrypted messages comprising the steps of: determining if a derived modulus N.sub.d is a squarefree

number, and if so, decrypting on a computer ciphertext C into message M wherein message M was originally an encrypted message that is transformed into electronic, decrypted message M using any method that produces a value equivalent to M=C.sup.d mod N.sub.d, where d is generated using the following steps: calculating the number Z.sub.d as the product of each prime factor of N.sub.d minus 1, (N.sub.d1-1)* . . . (N.sub.dj-1) for distinct prime factors of N.sub.d 1 to j, where j is the number of distinct prime factors in N.sub.d; generating the exponent d such that the following relationship is satisfied: e*d=1 mod Z.sub.d (Fig.1-5, and col.13 line 45 to col.17 line 15).

6. Regarding Claim 12, Takagi teach and describe a public key cryptosystem where messages are decrypted on a computer using a set of prime numbers S and the public exponent e, and messages are encrypted using a squarefree modulus N.sub.p that is calculated as the product of a set of distinct numbers that is a proper superset of S composed of distinct number, and encryption occurs with standard RSA methods using the public exponent e and the modulus N.sub.p (Fig.1-5, and col.13 line 45 to col.17 line 15).

7. Regarding Claim 13, Takagi teach and describe a method for encrypting/decrypting messages, comprising the steps of: Encrypting on a computer a plaintext message M into a ciphertext message C using any method that produces a value equivalent to C=M.sup.e mod N.sub.p, where 0.ltoreq.M<N such that the ciphertext C can be decrypted into the plaintext message M using e and the distinct prime factors of N, N being the product of all of the numbers

in the set S; N is not a squareful number; S being a set of at least one prime number, p.sub.1 . . . p.sub.k, where k is an integer greater than 0; S.sub.p being a proper superset of S composed of distinct prime numbers; N.sub.p being the product of all of the numbers in the set S.sub.p; e being a number (Fig.1-5, and col.13 line 45 to col.17 line 15).

9. Regarding Claim 19, Takagi teach and describe a method of decrypting encrypted messages, including the steps of: Decrypting on a computer the ciphertext message C into the plaintext message M by: determining if the modulus N is a squarefree number; and if so then, decrypting ciphertext C into message M using any method that produces a value equivalent to M=C.sup.d mod N, where d is generated using the following steps: Calculating the number Z as the product of each prime factor of N minus 1, (N.sub.1-1)* . . . (N.sub.j-1) for prime factors of N 1 to j, where j is the number of distinct prime factors in N; then generating the decryption exponent d such that the following relationship is satisfied: e*d=1 mod Z (Fig.1-5, and col.13 line 45 to col.17 line 15).

10. Regarding Claim 23, Takagi teach and describe a method for encrypting/decrypting messages comprising the steps of: Encrypting on a computer a plaintext message M into a ciphertext message C using any method that produces a value equivalent to C=M.sup.e mod N.sub.p, where 0.ltoreq.M<N, such that the ciphertext C can be decrypted into the plaintext message M using e and the prime factors of N. N being the product of all of the members of set S; N is not a squareful number; S being a set of at least two numbers, p.sub.1 . . . p.sub.k where k is an integer greater than 1 and all members of S are equal to p.sub.s, which is a prime number;

S.sub.p being a superset of S composed of distinct prime numbers; N.sub.p being the product of all of the numbers in the set S.sub.p; e being a number (Fig.1-5, and col.13 line 45 to col.17 line 15).

12. Regarding Claim 27, Takagi teach and describe a method for encrypting/decrypting messages, comprising the steps of: Encrypting on a computer a plaintext message M into a ciphertext message C using any method that produces a value equivalent to C=M.sup.e mod N.sub.p, where 0.ltoreq.M<p, such that the ciphertext C can be decrypted into the plaintext message M using e and p p being a prime number; S being a set containing only the number p; S.sub.p being a superset of S; consisting of distinct prime numbers N.sub.p being the product of all members of the set S.sub.p; N.sub.p is not a squareful number; e being a number (Fig.1-5, and col.13 line 45 to col.17 line 15).

13. Regarding Claim 30, Takagi teach and describe a method for decrypting encrypted messages, comprising the steps of: Decrypting on a computer using any method that produces a value equivalent to as M=C.sup.d mod p, where p is not a squareful number and d is generated using the following step: Calculating d such that the following equation is satisfied:e*d=1mod(p-1)- (Fig.1-5, and col.13 line 45 to col.17 line 15).

13. Regarding Claim 31, Takagi teach and describe a method for establishing cryptographic communications, comprising the steps of: calculating a composite number N, which is formed from the product of distinct prime numbers S, p.sub.1, . . . p.sub.k where k.gtoreq.1. and N is not

a squareful number; on a computer Encoding a plaintext message M, to a ciphertext C, where M corresponds to a number representative of a message and 0.ltoreq.M<S; generating an exponent e; transforming on a computer said plaintext, M, into said ciphertext, C, where C is developed using any method that produces a value equivalent to C=M.sup.e mod N, such that ciphertext C can be decrypted into plaintext M using only e and S (Fig.1-5, and col.13 line 45 to col.17 line 15).

14. Regarding Claim 34, Takagi teach and describe a method for decrypting encrypted messages, comprising the steps of: decoding on a computer the ciphertext message C to the plaintext message M, wherein said decoding comprises the step of: transforming said ciphertext message C to plaintext M, using any method that produces a value equivalent to M=C.sup.d mod S, where S is not a squareful number and d is generated using the following step: generating d such that e*d=1 mod (S-1) (Fig.1-5, and col.13 line 45 to col.17 line 15).

15. Regarding Claim 35, Takagi teach and describe a system for encrypting and decrypting electronic communications including a network of computers and/or computer-type devices, such as personal data assistants (PDAs), mobile phones and other devices, in particular mobile devices capable of communicating on the network; generating at least one private key and at least one public key, wherein the at least one private key is determined based upon any one of a multiplicity of prime numbers that when multiplied together produce N, which is the modulus for at least one of the public keys, and wherein the modulus N is not a squareful number (Fig.1-5, and col.13 line 45 to col.17 line 15).

16. Regarding Claim 36, Takagi teach and describe a method for public key decryption where less than all of the distinct prime factors of a number N are used to decrypt a ciphertext message C into plaintext message M, where encryption on a computer occurs with the public key {e, N} using any method that produces a value equivalent to C=M.sup.e mod N and N is not a squareful number (Fig.1-5, and col.13 line 45 to col.17 line 15).

17. Regarding Claim 37, Takagi teach and describe a method for public key encryption with a public key {e, N} where a plaintext message M is encrypted on a computer into a ciphertext message C using any method that produces a value equivalent to C=M.sup.e mod (N*X), where N is the public modulus wherein N is not a squareful number; and X is any integer greater than 1 (Fig.1-5, and col.13 line 45 to col.17 line 15).

18. Regarding Claim 38, Takagi teach and describe a method for public key decryption of a message that has been encrypted with the public key {e, N} where a ciphertext message C is decrypted on a computer into a plaintext message M using any method that produces a value equivalent to M=C.sub.d mod N.sub.d, where N.sub.d is the product of less than all of the prime factors of the public modulus N and d satisfies the equation e*d=1 mod Z, where Z is the product of each of the k prime factors of N.sub.d minus 1, (p.sub.1-1)* . . . (p.sub.k-1) and wherein the modulus N is not a squareful number (Fig.1-5, and col.13 line 45 to col.17 line 15).

19. Regarding Claim 39, Takagi teach and describe a method for public key decryption of a

message that has been encrypted on a computer using any method that produces a value equivalent to C=M.sup.e mod N, where a ciphertext message C is decrypted into a plaintext message M using any method that produces a value equivalent to M=C.sup.d mod N.sub.d, where N.sub.d is the product of less than all of the prime factors of the public modulus N and d satisfies the equation e*d=1 mod Z, where Z is the product of each of the k prime factors of N.sub.d minus 1, (p.sub.1-1)* . . . (p.sub.k-1) and wherein the modulus N is not a squareful number (Fig.1-5, and col.13 line 45 to col.17 line 15).

20. Claims 4, 6-8, 14-15, 20-22, 24-25, 28-29, and 32-33 are rejected applied as above rejecting Claims, 3, 5, 9, 13, 19, 27, and 31. Furthermore, Takagi teach and describe a public key cryptographic system and method wherein:

As per Claim 4, the step of generating the exponent e includes calculating the exponent e as a number that is relatively prime to the product of each distinct prime factor of N minus 1, (N.sub.1-1)* . . . (N.sub.j-1) for distinct prime factors of N 1 to j, where j is the number of distinct prime factors in N, or choosing the exponent e as a small prime number (col.9 line 5 to col.11 line 45).

As per Claim 6, further including the step of: directly calculating M=C.sup.d mod N.sub.d ((col.9 line 5 to line 65).

As per Claim 7 further including the steps of: calculating separate decryption exponents d.sub.ndl . . . d.sub.ndj for all prime factors of N.sub.d 1 to j, where j is the number of prime factors in N.sub.d so that the following relationship is satisfied for each member of N.sub.d:

e*d.sub.ndi=1 mod (N.sub.di-1); and performing decryptions of the form M.sub.i=C.sup..sub.dndi mod N.sub.di for all prime factors of N.sub.d from 1 to j, where j is the number of prime factors in N.sub.d, and then using the values of each M.sub.i and N.sub.di to reconstruct M (col.9 line 5 to col.11 line 45).

As per Claim 8, the values of each M.sub.i and N.sub.di restore the plaintext message M using the Chinese Remainder Theorem and/or Gamer's algorithm (col.9 line 5 to col.11 line 45).

As per Claim 14, the step of generating the exponent e includes calculating the exponent e as a number that is relatively prime to the product of each distinct prime factor of N.sub.p minus 1, (N.sub.p-1)* . . . (N.sub.pj-1) for distinct prime factors of N.sub.p 1 to j, where j is the number of distinct prime factors in N.sub.p (col.9 line 5 to col.11 line 45).

As per Claim 15, the step of generating the exponent e includes choosing the exponent e as a small prime number (col.3 line 46 to 4 line 14).

As per Claim 20, further including the step of: directly calculating M=C.sup.d mod N (col.9 line 5 to col.11 line 45).

As per Claim 21, further including the steps of: calculating separate decryption exponents d.sub.1 . . . d.sub.j for all prime factors of N 1 to j, where j is the number of prime factors in N so that the following relationship is satisfied for each member of N: e*d.sub.i=1 mod (N.sub.i-1); and performing decryptions of the form M.sub.i =C.sup..sub.di mod N.sub.i for all prime factors of N from 1 to j, where j is the number of prime factors in N, and then using the values of each M.sub.i and N.sub.i to reconstruct M (col.9 line 5 to col.11 line 45).

As per Claim 22, the values of each M.sub.i and N.sub.i reconstruct M using the Chinese Remainder Theorem and/or Garner's algorithm (col.9 line 5 to col.11 line 45).

As per Claim 24, the step of generating the exponent e further includes: Calculating the exponent e as a number that is relatively prime to the product of all of the distinct prime factors of N.sub.p minus 1, (N.sub.p-1)* . . . (N.sub.pj-1) for distinct prime factors of N.sub.p 1 to j, where j is the number of distinct prime factors in N.sub.p (col.9 line 5 to col.11 line 45).

As per Claim 25, the step of generating the exponent e includes choosing the exponent e as a small prime number (col.3 line 46 to 4 line 14).

As per Claim 28, the step of generating the exponent e further includes: Calculating the exponent e as a number that is relatively prime to the product of each distinct prime factor of N.sub.p minus 1, (N.sub.p1-1)* . . . (N.sub.pj-1) for distinct prime factors of N.sub.p 1 to j, where j is the number of distinct prime factors in N.sub.p (col.9 line 5 to col.11 line 45).

As per Claim 29, the step of generating the exponent e includes choosing the exponent e as a small prime number (col.3 line 46 to 4 line 14).

As per Claim 32, the step of generating the exponent e further includes: Calculating the exponent e as a number that is relatively prime to the product of each distinct prime factor of N minus 1, (N.sub.1-1), . . . (N.sub.j-1) for distinct prime factors of N 1 to j, where j is the number of distinct prime factors in N (col.9 line 5 to col.11 line 45).

As per Claim 33, the step of generating the exponent e includes choosing the exponent e as a small prime number (col.3 line 46 to 4 line 14).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
September 24, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431